Microsoft

# Microsoft Azure Sentinel

Planning and implementing Microsoft's cloud-native SIEM solution

Yuri Diogenes
Nicholas DiCola
Jonathan Trull

Foreword by Ann Johnson, Corporate Vice President – Cybersecurity Solutions at Microsoft

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Microsoft

# Microsoft Azure Sentinel

## Planning and implementing Microsoft's cloud-native SIEM solution

Yuri Diogenes
Nicholas DiCola
Jonathan Trull

# Microsoft Azure Sentinel

**Planning and implementing Microsoft's cloud-native SIEM solution**

**Published with the authorization of Microsoft Corporation by:**

**Pearson Education, Inc.**


ISBN-13: 978-0-13-648545-2
ISBN-10: 0-13-648545-6

Library of Congress Control Number: 2019957613

ScoutAutomatedPrintCode



For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

**CREDITS**

EDITOR-IN-CHIEF
Brett Bartow

EXECUTIVE EDITOR
Loretta Yates

DEVELOPMENT EDITOR
Rick Kughen

MANAGING EDITOR
Sandra Schroeder

SENIOR PROJECT EDITOR
Tracey Croom

COPY EDITOR
Rick Kughen

INDEXER
Valerie Perry

PROOFREADER
Vanessa Ta

TECHNICAL EDITOR
Maarten Goet

ASSISTANT SPONSORING EDITOR
Charvi Arora

EDITORIAL ASSISTANT
Cindy Teeters

COVER DESIGNER
Twist Creative, Seattle

COMPOSITOR
Happenstance Type-O-Rama

# Acknowledgments

The authors would like to thank Loretta Yates and the entire Microsoft Press/Pearson team for their support in this project, Ann Johnson for writing the foreword, and also the Azure Sentinel Engineering Team (Eliav Levi, Ofer Shezaf, Koby Koren, Raz Herzberg, Mor Shabi, Laura Machado de Wright, Ben Nick, Julian Gonzalez, and Itay Argoety). Thanks to Ian Hellen for the great work writing Chapter 6. We would also like to thank Maarten Goet (Microsoft MVP) for reviewing this book and thanks to Mike Kassis for writing the Appendix about Kusto Query Language (KQL).

Yuri would also like to thank: my wife and daughters for their endless support; my great God for giving me strength and guiding my path on each step of the way; my co-authors and friends Nicholas DiCola and Jonathan Trull for such great partnership throughout this project. Thanks to my parents for working hard to give me an education, which is the foundation I use every day to keep moving forward in my career. Last, but certainly not least, the entire Azure Sentinel community that keep inspiring us with great content.

Nicholas would also like to thank: my wife and three children for supporting me while working on this book; my co-authors and friends Yuri Diogenes and Jonathan Trull for their hard work on this book. I would also like to thank our Azure Sentinel Engineering team technical reviewers for their support on the book.

Jonathan would also like to thank: God, who is my ultimate teacher and guide; my wife and daughters for their love, encouragement, and endless support; my parents for providing me with the time and resources to pursue my dreams; my extended family for always believing in me; and my co-authors and comrades Yuri Diogenes and Nicholas DiCola. Finally, thanks to Microsoft, the Cybersecurity Solutions Group, and the countless teachers, professors, colleagues, and friends who have taught, counseled, and mentored me over the years.

# Contents at a Glance

# Contents

# About the Authors

**Yuri Diogenes, MsC**

Master of science in cybersecurity intelligence and forensics investigation (UTICA College), Yuri is Senior Program Manager in Microsoft Cxe Security Team, where he primarily helps customers onboard and deploy Azure Security Center and Azure Sentinel. Yuri has been working for Microsoft since 2006 in different positions, including five years as senior support escalation engineer in CSS Forefront Edge Team, and from 2011 to 2017 in the content development team, where he also helped create the Azure Security Center content experience since its launch in 2016. Yuri has published a total of 22 books, mostly around information security and Microsoft technologies. Yuri also holds an MBA and many IT/Security industry certifications, such as CISSP, E|CND, E|CEH, E|CSA, E|CHFI, CompTIA Security+, CySA+, Cloud Essentials Certified, Mobility+, Network+, CASP, CyberSec First Responder, MCSE, and MCTS. You can follow Yuri on Twitter at *@yuridiogenes*.

**Nicholas DiCola**

Nicholas is a Principal Group PM Manager at Microsoft on the Security Customer Experience Engineering (CxE) team, where he leads the Azure Security Get-To-Production team that helps customers with deployments of Azure Security products.  He has a Master of Business Administration with a concentration in Information Systems and various industry certifications such as CISSP and CEH.  You can follow Nicholas on Twitter at *@mastersecjedi*.

**Jonathan Trull**

Jonathan is Microsoft's Chief Security Strategist. He provides strategic direction on the development of Microsoft products and services and leads a team of security, compliance, and identity advisors who help customers secure their digital transformation initiatives. Jonathan is a seasoned security executive who formally served as the CISO for the State of Colorado and several commercial organizations. He is active in the security community and is helping lead the Cloud Security Alliance's cloud controls matrix working group and is a coach for Carnegie Mellon University's CISO Executive Program. You can follow Jonathan on Twitter at *@jonathantrull* or via LinkedIn at *https://www.linkedin.com/in/jonathantrull/*.

# Foreword

Security is—at its' core—a big data problem. Businesses and government entities are producing terabytes of security relevant log data every day and the volumes continue to increase. This data growth is driven by the digitization of business processes and an explosion in the number of intelligent devices being used to power our physical world. Security teams are charged with making sense of this data and spotting the signs of an active attack so that they can respond appropriately.

Azure Sentinel was purpose-built to help address the challenges faced by our customer's security operations teams. It was engineered as a cloud service to automatically scale to the data volumes thrown at it. This allows security teams to focus their time on identifying threats as opposed to administering infrastructure. Azure Sentinel also includes capabilities to automate responses to alerts by triggering playbooks. Playbooks can also collect and add context to existing alerts to speed decision making by SOC analysts.

Yuri, Nicholas, and Jonathan have been working with Azure Sentinel from the beginning of the design and engineering process and have successfully deployed Azure Sentinel for customers large and small. They lay out the foundational aspects of architecting and implementing Azure Sentinel, including connecting data sources; writing custom alerts, workbooks, and playbooks; and using the product to proactively hunt for threats. The authors not only cover the full breadth of product capabilities in the book, but they also offer their practical advice to ensure successful deployment.

Microsoft is fulfilling a mission to develop a robust portfolio of security, compliance, and identity products to meet the needs of our enterprise customers. The security, compliance, and identity solutions are fully integrated and leverage Microsoft's vast threat-intelligence sources to maximize their effectiveness. Azure Sentinel will be a cornerstone of the Microsoft portfolio for years to come and has already been quickly adopted across the globe by customers of all sizes.

*Microsoft Azure Sentinel* is the authoritative source for implementing Microsoft's hottest new security solution. It was a pleasure to review for Yuri, Nicholas, and Jonathan. Pick up your copy today!

Ann Johnson
Corporate Vice President
Cybersecurity Solutions Group

# Introduction

Welcome to Azure Sentinel. This book was developed together with the Azure Sentinel product group to provide in-depth information about Microsoft's new cloud-based security information and event management (SIEM) system, Azure Sentinel, and to demonstrate best practices based on real-life experience with the product in different environments.

The purpose of this book is to introduce the wide array of capabilities available in Azure Sentinel. After being introduced to the main use case scenarios to use Azure Sentinel, you will dig in to see how to deploy and operationalize Azure Sentinel for data collection, analytics, incident management, threat detection, and response.

# Who is this book for?

Azure Sentinel is for anyone interested in security operations in general: cybersecurity analysts, security administrators, threat hunters, support professionals, and engineers.

Azure Sentinel is designed to be useful for Azure and non-Azure users. You can have no security experience, some experience, or be a security expert and will get value from Azure Sentinel. This book provides introductory, intermediate, and advanced coverage on a large swath of security issues that are addressed by Azure Sentinel.

The approach is a unique mix of didactic, narrative, and experiential instruction. Didactic covers the core introductions to the services. The narrative leverages what you already understand, and we bridge your current understanding with new concepts introduced in the book.

Finally, the experience component is presented in two ways— we share our experiences with Azure Sentinel and how to get the most out of it by showing in a stepwise, guided fashion how to configure Azure Sentinel to gain all the benefits it has to offer.

In this book you will learn:

- How to connect different data sources to Azure Sentinel
- How to create security analytics
- How to investigate a security incident in Azure Sentinel
- System requirements
- Anyone with access to a Microsoft Azure subscription can use the information in this book.

## Errata, updates & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

*MicrosoftPressStore.com/AzureSentinel/errata*

If you discover an error that is not already listed, please submit it to us at the same page.

For additional book support and information, please visit *http://www.MicrosoftPressStore.com/Support*.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *http://support.microsoft.com*.

## Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

Chapter 2

# Introduction to Azure Sentinel

Given the threat landscape presented in Chapter 1, there is a clear need for a system that can collect data from different sources, perform data correlation, and present this data in a single dashboard.

Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response. Azure Sentinel natively incorporates proven foundation services from Azure, such as Log Analytics and Logic Apps. Also, Azure Sentinel enriches your investigation and detection with Artificial Intelligence (AI) in conjunction with Microsoft's threat intelligence stream.

In this chapter, you will learn more about the architecture, design considerations, and initial configuration of Azure Sentinel.

## Architecture

Because Azure Sentinel is part of Azure, the first prerequisite to deployment is to have an active Azure subscription. As with any other security information and event management (SIEM), Azure Sentinel needs to store the data that it will collect from the different data sources that you configure. Azure Sentinel will store this data in your preferred Log Analytics workspace. You can create a new workspace or use an existing one. However, it is recommended that you have a dedicated workspace for Azure Sentinel because alert rules and investigations do not work across workspaces. Keep in mind that you need at least contributor permission for the subscription in which the workspace resides.

> ***TIP*** **All the data you stream to Azure Sentinel is stored in the geographic location of the workspace you selected.**

To help you to better understand Azure Sentinel's architecture, you need to first understand the different components of the solution. Figure 2-1 shows a diagram of the major Azure Sentinel components.

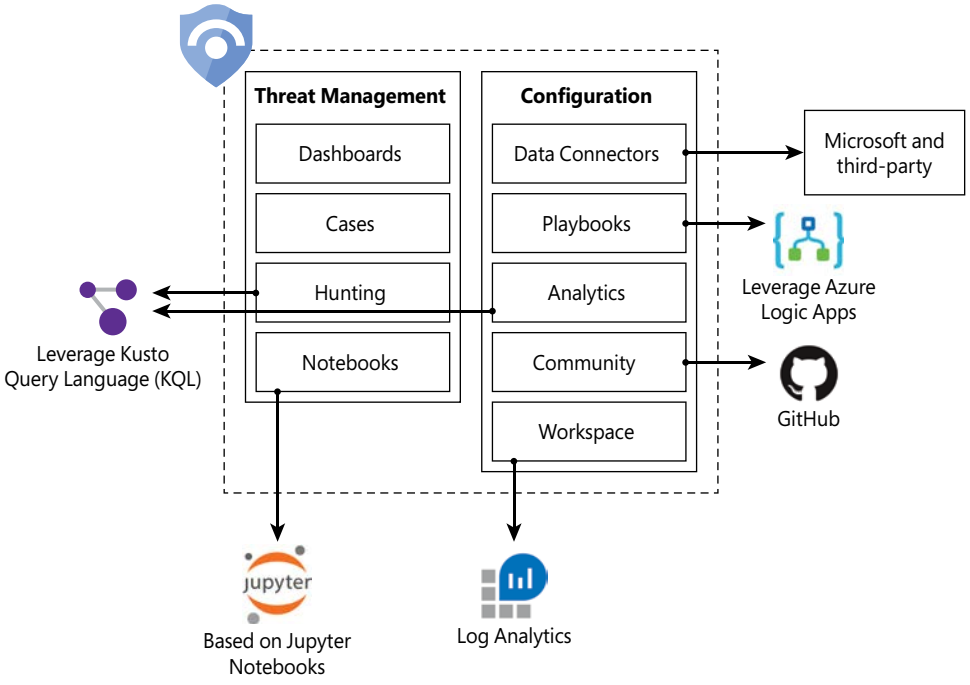


**FIGURE 2-1** Major components of Azure Sentinel

The components shown in Figure 2-1 are presented in more detail below:

- **Dashboards**: Built-in dashboards provide data visualization for your connected data sources, which enables you to deep dive into the events generated by those services. You will learn more about dashboards in Chapter 8, "Data visualization."
- **Cases**: A case is an aggregation of all the relevant evidence for a specific investigation. It can contain one or multiple alerts, which are based on the analytics that you define. You will learn more about cases in Chapter 4, "Case management."
- **Hunting:** This is a powerful tool for investigators and security analysts who need to proactively look for security threats. The searching capability is powered by Kusto Query Language (KQL). You will learn more about hunting in Chapter 5, "Hunting."
- **Notebooks:** By integrating with Jupyter notebooks, Azure Sentinel extends the scope of what you can do with the data that was collected. The notebooks feature combines full programmability with a collection of libraries for machine learning, visualization, and data analysis. You will learn more about notebooks in Chapter 6, "Notebooks."
- **Data Connectors:** Built-in connectors are available to facilitate data ingestion from Microsoft and partner solutions. You will learn more data connectors later in this chapter.
- **Playbooks:** A Playbook is a collection of procedures that can be automatically executed upon an alert triggered by Azure Sentinel. Playbooks leverage Azure Logic Apps, which help you automate and orchestrate tasks/workflows. You will learn more about playbooks in Chapter 7, Automation with Playbooks."

- **Analytics:** Analytics enable you to create custom alerts using Kusto Query Language (KQL). You will learn more about analytics in Chapter 3, "Analytics."
- **Community:** The Azure Sentinel Community page is located on GitHub, and it contains Detections based on different types of data sources that you can leverage in order to create alerts and respond to threats in your environment. The Azure Sentinel Community page also contains hunting query samples, playbooks, and other artifacts. You will learn more about community in Chapter 3, "Analytics."
- **Workspace:** Essentially, a Log Analytics workspace is a container that includes data and configuration information. Azure Sentinel uses this container to store the data that you collect from the different data sources. You will learn more about workspace configuration later in this chapter.

## Adoption considerations

Although Azure Sentinel is a cloud-based SIEM, there are some initial design considerations that you must be aware of. When planning Azure Sentinel adoption, use the following list of questions as the foundation for your initial assessment. This will help you to identify the areas from which you need to obtain more details before deploying Azure Sentinel:

1. **Who has permission to deploy Azure Sentinel in my tenant?**
   - Azure Sentinel uses a Role-Based Access Control model and enables you to set granular levels of permissions for different needs. There are three built-in roles available for Azure Sentinel, they are:
     - Azure Sentinel reader: enable the user to view incidents and data but cannot make changes.
     - Azure Sentinel responder: enable the user to read and perform some actions on incidents, such as assign to another user or change the incident's severity.
     - Azure Sentinel contributor: enable the user to read, perform some actions on incidents and create or delete analytic rules.

   To deploy Azure Sentinel on your tenant you need contributor permissions to the subscription in which the Azure Sentinel workspace resides.

   Note: All Azure Sentinel built-in roles grant read access to the data in your Azure Sentinel workspace.
2. **What permissions do the team members require to do their jobs using Azure Sentinel?**
   - It is important to plan who will have access to the Azure Sentinel Dashboard. Depending on how the organization is structured, you may have different teams handling different areas of Azure Sentinel. For example, the SecOps team might be actively looking at new alerts, while the Threat Hunting Team might be performing proactive hunting. Again, leverage the RBAC model to assign granular permissions to different groups.
   - Consider the different scenarios, such as creating cases, closing cases, creating new analytics, using hunting queries, and writing playbooks.

3. **Am I going to deploy Azure Sentinel in a single or multitenant scenario?**
   - Azure Sentinel can be deployed in both scenarios. In a multitenant scenario, you can deploy Azure Sentinel on each tenant and use Azure Lighthouse to have a multitenant visualization of all tenants.
4. **What are the data sources from which I want to ingest data?**
   - That's probably one of the most critical questions to ask in the beginning of the project. By having a list of data sources that you want to connect to Azure Sentinel, you can evaluate whether there are built-in connectors for the target system or whether you will need to use another method to connect. Here, you should also define whether you are going to ingest data only from cloud resources or if you also plan to collect data from on-premises resources.
   - Make sure to prioritize the data sources that are more important for your business. If you are just performing a proof-of-concept, ensure that you connect to the primary Microsoft services that are used by your organization and at least a couple of on-premises resources that will be utilized in production.
5. **Do I already have Azure Security Center deployed and monitoring my servers?**
   - If you already have Azure Security Center deployed and you are using the default workspace created by Security Center, you need to be aware that you can't enable Azure Sentinel on this default workspace. However, if you are using a custom workspace in Azure Security Center, you can enable Azure Sentinel on this workspace. You will find more details about workspace design in "Enabling Azure Sentinel," later in this chapter.

These are key questions that you must answer before you start configuring Azure Sentinel. Once you answer these questions—and others that may be very specific to your type of organization—you are ready to enable Azure Sentinel in your Azure subscription.

## Enabling Azure Sentinel

Azure Sentinel is available in Azure Portal, and to enable it, you need a Log Analytics workspace. A Log Analytics workspace provides:

- A geographic location for data storage.
- Data isolation by granting different users access rights following the Log Analytics' recommended design strategies for workspaces; these recommendations can be found at *http://aka.ms/asbook/workspacedesign*.
- A scope for configuration of settings, such as pricing tier, retention, and data capping.

Although Azure Sentinel supports multiple workspaces for some scenarios, it is recommended that you use a centralized workspace because alert rules and investigations do not function across workspaces.

> ***NOTE*** **To learn more about workspace design consideration and Role-Base Access Control (RBAC) for workspaces, visit *http://aka.ms/asbook/workspaces* and *http://aka.ms/asbook/workspacesbp*.**

The following steps assume that you don't have a workspace and that you will create one as part of the Azure Sentinel deployment:

6. Open **Azure Portal** and sign in with a user who has contributor privileges in the subscription in which the Azure Sentinel workspace resides.
7. Under **All services**, type *Sentinel* and click **Azure Sentinel,** as shown in Figure 2-2.

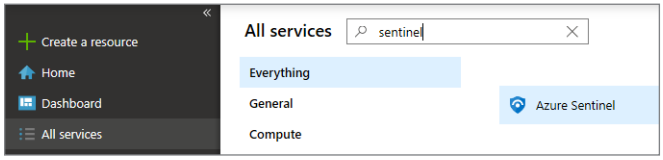


**FIGURE 2-2** Accessing Azure Sentinel in Azure Portal

8. When Azure Sentinel launches for the first time, there is no workspace associated to it; the initial blade will look similar to Figure 2-3.

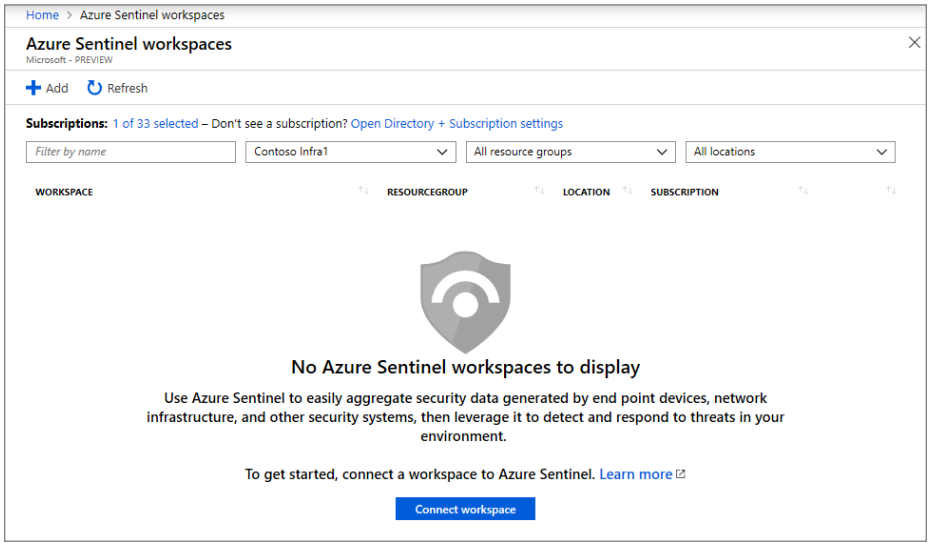


**FIGURE 2-3** Azure Sentinel workspace selection page

9. At this point, you can either click the **Add** button or click the **Connect Workspace** button. Both options will lead you to the **Choose a workspace to add to azure sentinel** page, as shown in Figure 2-4.

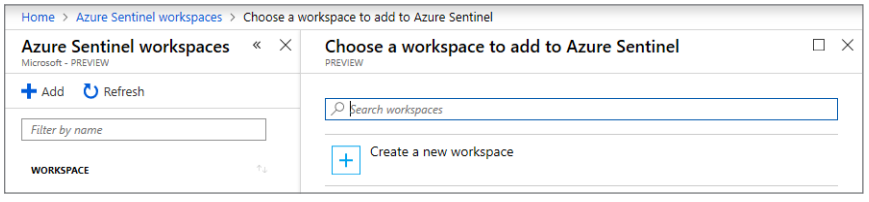


**FIGURE 2-4** Adding a new workspace to Azure Sentinel

10. Click the **Create a new workspace** option; the **Log analytics workspace** page appears, as shown in Figure 2-5.

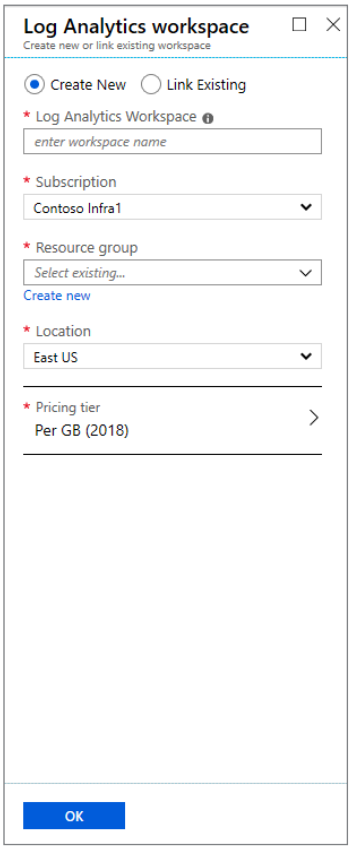


**FIGURE 2-5** Creating a new workspace to be used by Azure Sentinel

11. In the **Log Analytics Workspace** field, type a name for the workspace.
12. In the **Subscription** field, select the subscription that you want to use.
13. From the **Resource group** drop-down menu, select the resource group you want to use.
14. From the **Location** drop-down menu, select the location where the workspace will reside.
15. For the **Pricing tier**, select **Per GB**.
16. After completing those fields, click the **OK** button.
17. On the **Choose a workspace to add to Azure Sentinel** page, select the workspace that you just created and click the **Add Azure Sentinel** button; the initial **Azure Sentinel** dashboard appears, as shown in Figure 2-6.

Now that you have your workspace configured, you are ready to start ingesting data from different sources. We'll cover that in the next section.

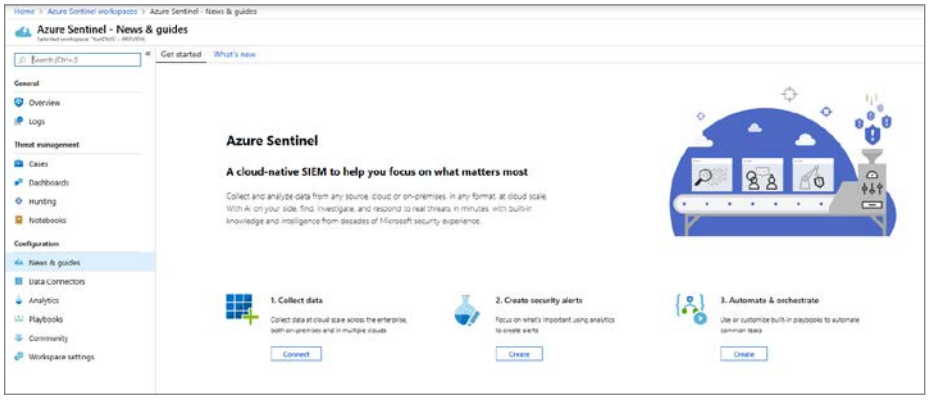


**FIGURE 2-6** Initial Azure Sentinel page

## Data ingestion

Azure Sentinel enables you to use data connectors to configure connections with different Microsoft services, partner solutions, and other resources. There are several out-of-the-box data connectors available in Azure Sentinel, and there are different ways to ingest data when a connector is not available. Figure 2-7 shows a diagram of the available options.

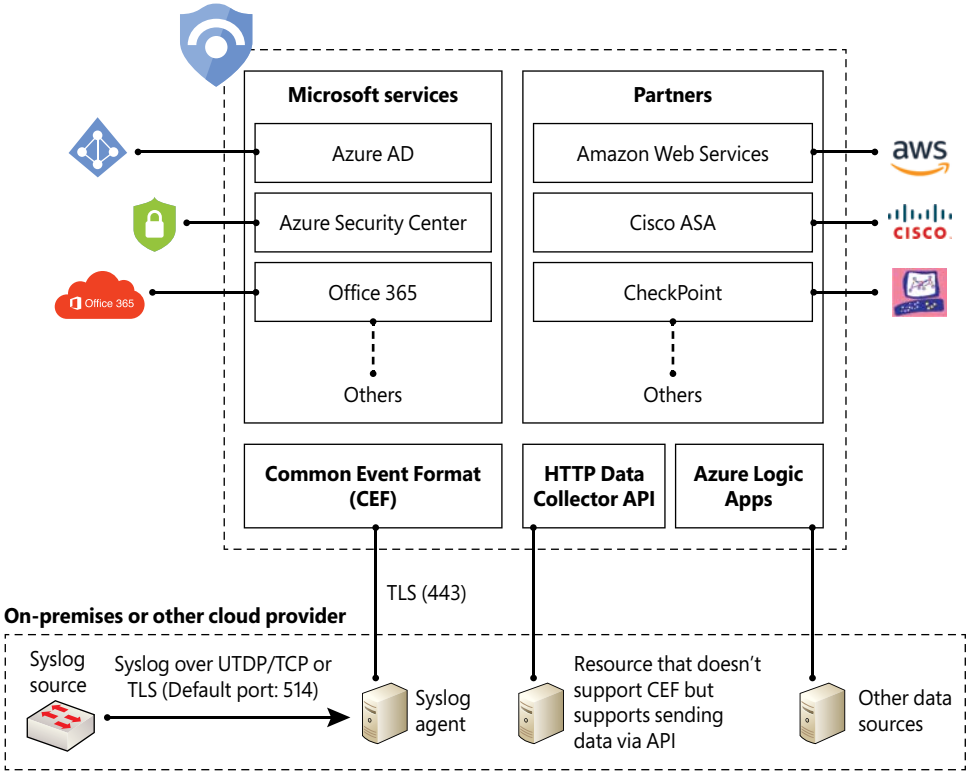


**FIGURE 2-7** Different methods to ingest data into Azure Sentinel

Figure 2-7 only shows a small subset of Microsoft services. At the time this chapter was written, Azure Sentinel provided support for the following Microsoft services:

- Azure AD
- Office 365
- Cloud App Security
- Azure Activity Log
- Azure AD Identity Protection
- Azure Information Protection
- Azure ATP
- Azure Security Center
- Domain Name Server
- Microsoft Defender ATP
- Microsoft Web Application Firewall
- Windows Firewall
- Windows Security Events

The diagram also shows a subset of partners' connectors. The number of connectors may change over time as Microsoft continues to encourage other vendors to partner and create new connectors. At the time this chapter was written, the following external connectors were available:

- Amazon Web Services (AWS)
- Barracuda
- Check Point
- Palo Alto Networks
- Fortinet
- F5
- Symantec ICDX

If an external solution is not on the data connector list, but your appliance supports saving logs as Syslog Common Event Format (CEF), the integration with Azure Sentinel is available via CEF Connector. If CEF support is not available on your appliance, but it supports calls to a REST API, you can use the HTTP Data Collector API to send log data to the workspace on which Azure Sentinel is enabled. Data ingestion from some of these connectors requires a license, while some others are free. To see an updated pricing list for the connectors, visit *http://aka.ms/asbook/dataconnectors*.

> ***TIP*** **To learn how to use the HTTP Data Collector API to send log data to a workspace from a REST API client, visit *http://aka.ms/asbook/datacollectorapi*.**

### Utilize a cloud-native SIEM to reduce integration costs and free up resources

Ease of integration with telemetry sources is key to SIEM success. I often encounter security operations teams that spend too much effort on connecting data sources and maintaining event flow, which reduces the time they spend delivering security value. The cloud environment enables Azure Sentinel to offer a resilient and straightforward way to connect to data sources; this is done by abstracting servers and networks and by offering service-based serverless computing.

For example, with just a few clicks, you can connect Sentinel to Office 365, Azure AD, or Azure WAF and start receiving events immediately and get populated dashboards in minutes. Now that you are connected, there is no need to worry about connectivity health. No collector machine can fail or be choked with an event spike.

If an Office 365 customer is struggling with the implementation of detection use cases to address auditor concerns, they will find that a month-long project using a legacy SIEM can be implemented in less than a day by onboarding Azure Sentinel, connecting it to Office 365, and implementing the required use cases.

You may think that this is true only for collecting from Microsoft sources; however, Azure Sentinel AWS CloudTrail connector, which is based on serverless cloud-to-cloud connection, provides the same benefits. Connect in a few clicks and never worry about a failing VM or event spike.

Collecting from on-premises systems tends to require legacy collection methods such as Syslog. However, vendors such as F5, Symantec, and Barracuda offer native integration of their systems to Azure Sentinel providing the cloud-native collection benefits to on-premises equipment.

**Ofer Shezaf, Principal Program Manager, Azure Sentinel Team**

## Ingesting data from Microsoft solutions

One way to quickly start validating Azure Sentinel's data ingestion is to start the configuration by using Microsoft built-in connectors. To visualize data from the subscription-level events that have occurred in Azure—which includes data ranging from Azure Resource Manager (ARM)

operational data to updates on service health events—you can start with Azure Activity Log. Follow the steps below to connect with Azure Activity Log:

1. Open **Azure Portal** and sign in with a user who has contributor privileges for the workspace on which Azure Sentinel will be enabled and the resource group.
2. Under the **All services** option, type *Sentinel* and click **Azure Sentinel** when it appears at the lower right, as shown in Figure 2-8.

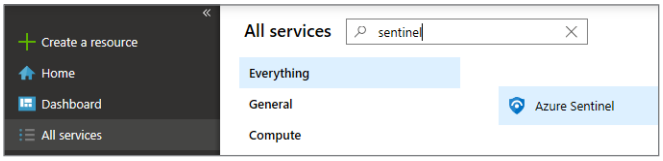


**FIGURE 2-8** Accessing Azure Sentinel in Azure Portal

3. Click in the workspace that was created in the "Enabling Azure Sentinel" section, earlier in this chapter.
4. When the **Azure Sentinel** dashboard opens, click **Data Connectors** under **Configuration** in the left navigation pane.
5. From the list of connectors, click **AzureActivity**; the **AzureActivity** page will appear, as shown in Figure 2-9.

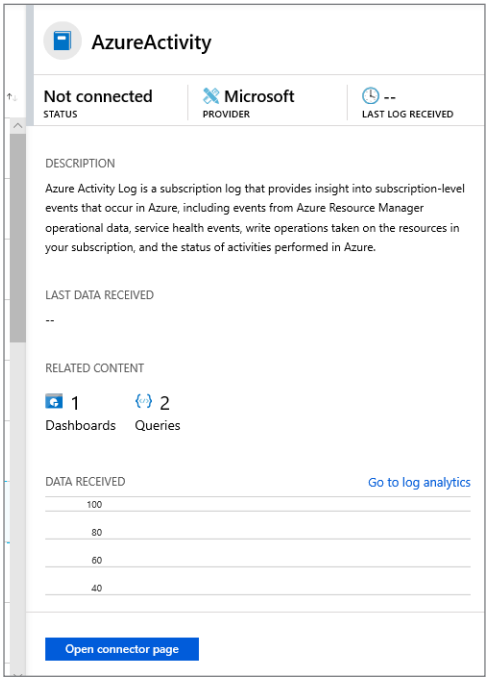


**FIGURE 2-9** Azure Activity Log connector blade

6. Click the **Open Connector Page** button, and you will see the **Instructions** tab, as shown in Figure 2-10.

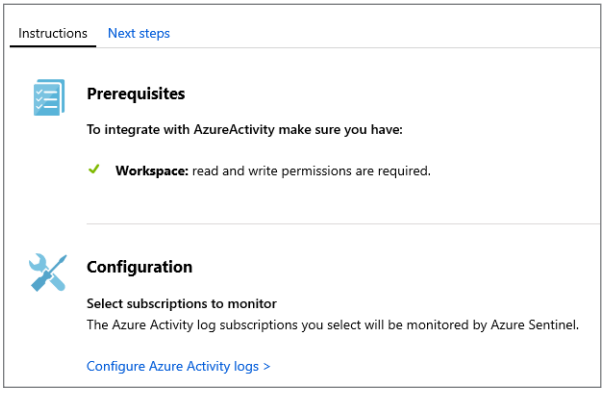


**FIGURE 2-10** Instructions tab with more details about prerequisites and configuration

7. Click the **Configure Azure Activity logs** option, and the Azure Activity Log page appears. Click the subscription to which you want to connect and click the **Connect** button.
8. Wait until you see a notification indicating the subscription was successfully connected and click the **Refresh** button. Ensure that the status has changed to Connected and close each blade until you see the main **Data Connectors** page.
9. Click **Overview** under **General** in the left navigation pane.
10. On the **Overview** page, you will see that there is no activity yet; this is expected because you just initiated the ingestion of Azure Activity Logs. Now you will generate some activity, and at the end of this chapter, you will check how the data flowed to Azure Sentinel. Create a new Virtual Machine with the following specifications:
    - **Operating System:** Windows Server 2016.
    - **Resource Group:** Use the same resource group that you created for the workspace in the "Enabling Azure Sentinel" section, earlier in this chapter.
    - **Remote Desktop Connection:** Enabled.

## Connecting to Azure Security Center

If you have Azure Security Center enabled in your subscription, you can start ingesting the Security Alerts generated by Security Center, which provides a rich set of threat detections. Security Center will generate alerts according to the different resource types:

- Infrastructure as a Service (IaaS), Virtual Machines (VMs), and non-Azure servers
- Native compute
- Data services

You need the Azure Security Center standard tier in order to connect with Azure Sentinel. Follow the steps below to connect to Security Center and start streaming security alerts to Azure Sentinel:

1. Open **Azure Portal** and sign in with a user who has contributor privileges for the workspace on which Azure Sentinel will be enabled as well as the resource group.
2. Under the **All services** option, type *Sentinel*, and click **Azure Sentinel,** as shown in Figure 2-11.

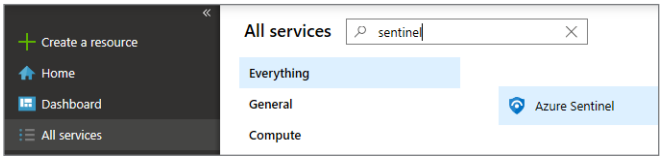


**FIGURE 2-11** Accessing Azure Sentinel in Azure Portal

3. Click in the workspace that was created in the "Enabling Azure Sentinel" section, earlier in this chapter.
4. When the **Azure Sentinel** dashboard opens, click **Data Connectors** under **Configuration** in the left navigation pane.
5. Click **Azure Security Center**, and a new pane appears on the right side, as shown in Figure 2-12.

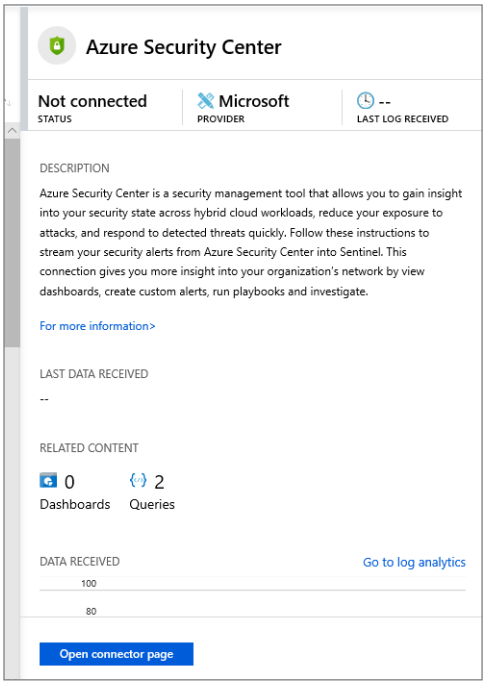


**FIGURE 2-12** Azure Security Center connector

6. Click **Open Connector Page** button and the full Azure Security Center connector page appears, as shown in Figure 2-13.

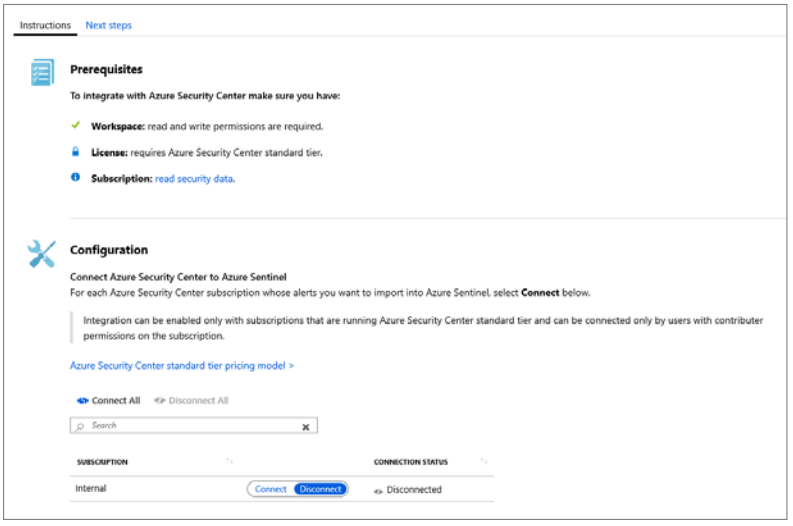


**FIGURE 2-13** Azure Security Center connector page

7. Under the **Configuration** section, next to the subscription that has the Azure Security Center standard tier enabled, click **Connect**.
8. The **Connection Status** will temporarily appear as Connecting, and once it is finished, it will appear as Connected.
9. After confirming that it is connected, close the Azure Security Center page, and on the **Data Connectors** page, click **Refresh;** you will see that the Azure Security Center connector status appears as Connected, as shown in Figure 2-14.


**FIGURE 2-14** Azure Security Center connector fully connected

10. Click the **Overview** option in the left pane to return to the main dashboard.

> ***TIP*** **If you want to generate some alerts in Azure Security Center, you can use the set of instructions available in the Security Center playbooks at *http://aka.ms/ascplaybooks*.**

## Connecting to Azure Active Directory

Azure Active Directory (Azure AD) is the identity and access-management service in the cloud. Each Azure tenant has a dedicated and trusted Azure AD directory. The Azure AD directory includes the tenant's users, groups, and apps, and it is used to perform identity and access-

management functions for tenant resources. If you want to export sign-in data from Active Directory to Azure Sentinel, you must have an Azure AD P1 or P2 license.

To connect Azure Sentinel with Azure AD, follow these steps:

1. Open **Azure Portal** and sign in with a user who has global administrator or security administrator permissions. You also need to have read permission to access Azure AD diagnostic logs if you want to see connection status.
2. Choose the **All services** option, type *Sentinel* in the search box, and click **Azure Sentinel,** as shown in Figure 2-15.

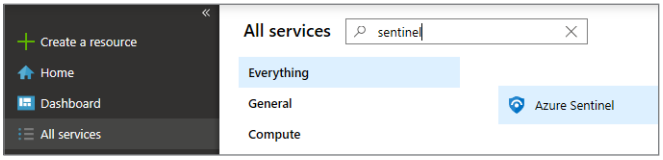


**FIGURE 2-15** Accessing Azure Sentinel in Azure Portal

3. Click the workspace that was created in the "*Enabling Azure Sentinel*" section, earlier in this chapter.
4. When the **Azure Sentinel** dashboard opens, click **Data Connectors** under **Configuration** in the left navigation pane.
5. Click **Azure Active Directory**, and a new pane appears on the right side, as shown in Figure 2-16.

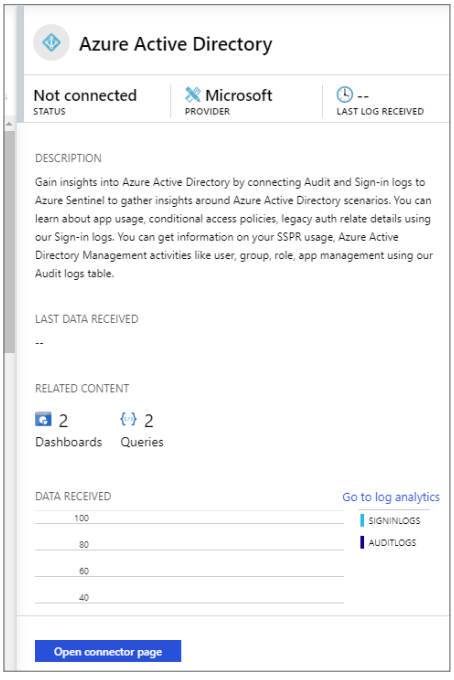


**FIGURE 2-16** Azure Active Directory connector

6. Click **Open Connector Page** button, and the full Azure Active Directory connector page appears, as shown in Figure 2-17.

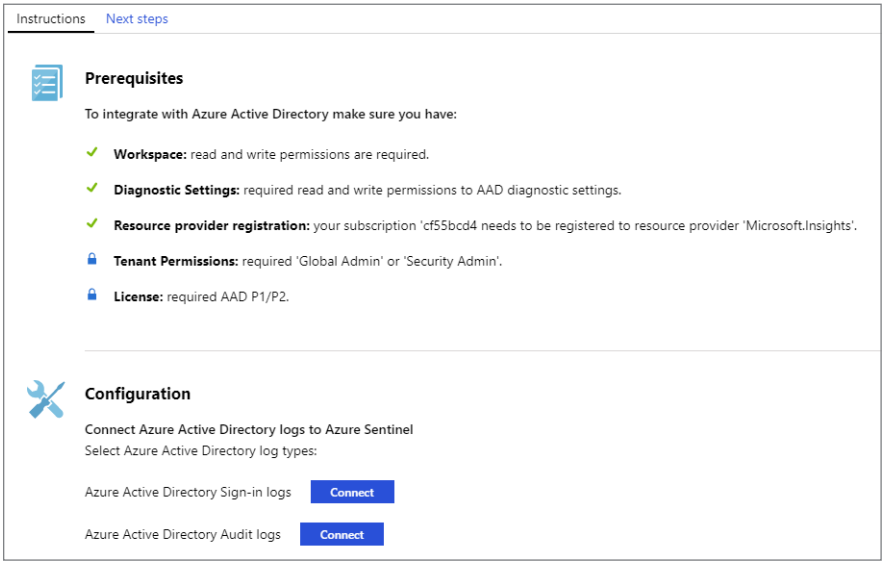


**FIGURE 2-17** Azure Active Directory connector page

7. In the **Configuration** section, you have the option to connect to Azure AD sign-in logs and audit logs. Ideally, you should connect with both because it provides a broader visibility of your identity related activities. For this example, click both **Connect** buttons.
8. Once you finish connecting, both buttons will change to **Disconnect**.
9. Close this page and click the **Overview** option in the left pane to return to the main dashboard.

## Connecting to Azure Active Directory Identity Protection

Azure Active Directory Identity Protection helps to protect your organization's identities by enabling you to configure risk-based policies that automatically respond to detected issues when a specified risk level has been reached. To perform the integration of Azure Active Directory Identity Protection with Azure Sentinel, you must have an Azure Active Directory Premium P1 or P2 license.

To connect Azure Sentinel with Azure Active Directory Identity Protection, follow these steps:

1. Open **Azure Portal** and sign in with a user who has global administrator or security administrator permissions.

2. In the **All services** text box, type *Sentinel*, and click **Azure Sentinel** when it appears as the lower right, as shown in Figure 2-18.

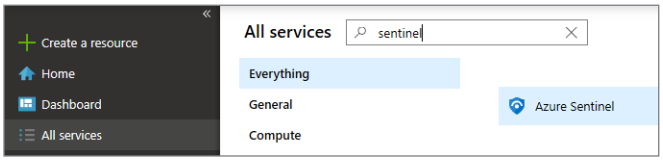


**FIGURE 2-18** Accessing Azure Sentinel in Azure Portal

3. Click the workspace that was created in the "*Enabling Azure Sentinel*" section, earlier in this chapter.
4. When the **Azure Sentinel** dashboard opens, click **Data Connectors** under **Configuration** in the left navigation pane.
5. Click **Azure Active Directory Identity Protection**, and a new pane appears on the right side, as shown in Figure 2-19.

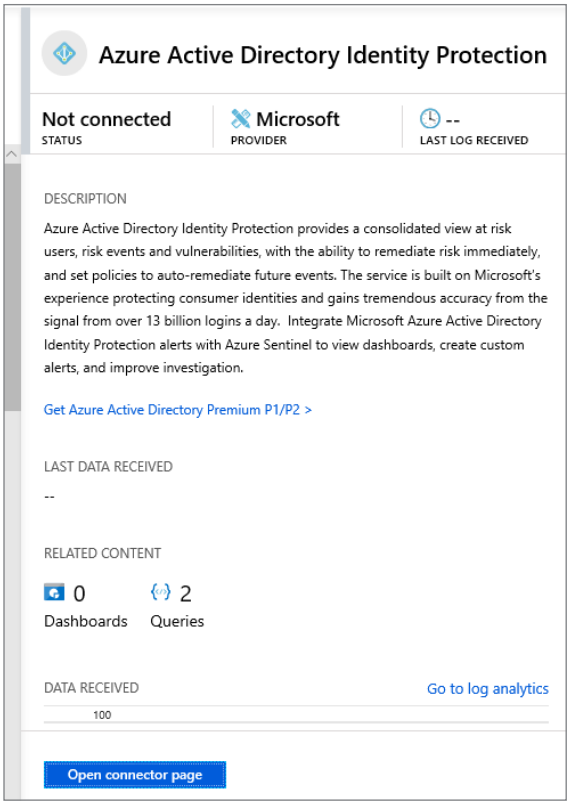


**FIGURE 2-19** Azure Active Directory Identity Protection connector

6. Click the **Open Connector Page** button and the full Azure Active Directory Identity Protection connector page appears, as shown in Figure 2-20.

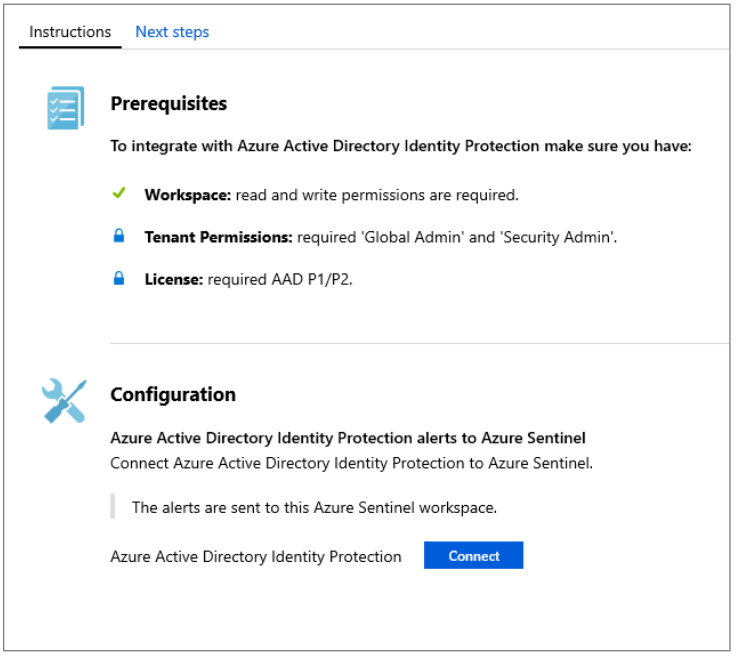


**FIGURE 2-20** Azure Active Directory Identity Protection connector

7. Under **Configuration**, click the **Connect** button.
8. Once you finish connecting, the button will change to **Disconnect**.
9. Close this page and click the **Overview** option in the left pane to return to the main dashboard.

There are many more connectors for other Microsoft Solutions, and most of them follow the same flow as the solutions explained so far. The only thing you need to be aware of are the prerequisites for each solution. Make sure to visit the product's webpage to better understand what permissions are necessary to connect to the target data set. In Chapter 9, "Integrating with partners," you will learn how to connect with some partners' solutions.

## Accessing ingested data

After connecting with the data sources that you need, you can start validating the connection flow to ensure the data is being saved in the workspace. To perform this validation, you need to access the workspace from Azure Sentinel and perform some queries using Kusto Query Language (KQL).

A Kusto query is a read-only request to process data and return results. The request is stated in plain text, using a data-flow model designed to make the syntax easy to read, author, and automate. The query uses schema entities that are organized in a hierarchy similar to SQL's databases, tables, and columns.

Follow these steps to access the workspace from Azure Sentinel and perform the validation for Azure Activity Log, which was the first data source that you connected in this chapter:

1. Open **Azure Portal** and sign in with a user who has contributor privileges for the workspace in which Azure Sentinel will be enabled as well as contributor privileges for the resource group.
2. Select the **All services** option, type *Sentinel*, and click **Azure Sentinel,** as shown in Figure 2-21.

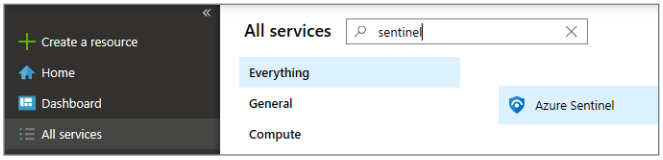


**FIGURE 2-21** Accessing Azure Sentinel in Azure Portal

3. Click in the workspace that was created in the "*Enabling Azure Sentinel*" section, earlier in this chapter, and the **Azure Sentinel** main dashboard appears.
4. Under **General**, click **Logs**.
5. On the Logs page, type *AzureActivity* and click the **Run** button. You should see all activities that were performed and collected in the last 24 hours (which is the default timeframe). The result should look similar to Figure 2-22.

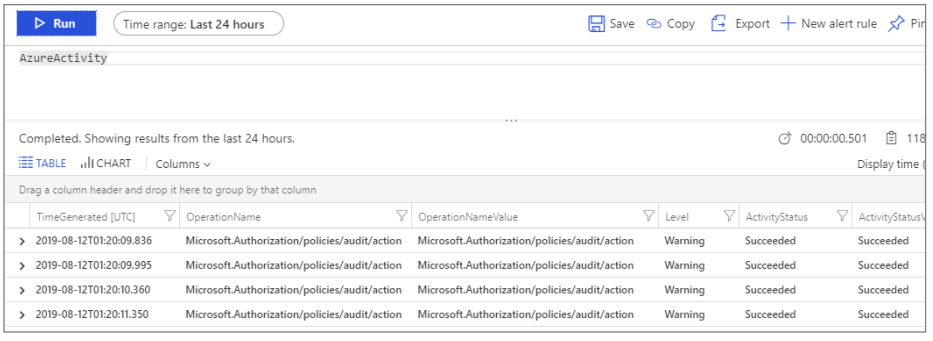


**FIGURE 2-22** Azure Sentinel workspace results

As you can see, the logs are flowing, and you can obtain all results with a single query. However, in a real scenario, you want to narrow the results. An easy way to learn KQL while performing queries is to leverage the context-sensitive IntelliSense capability. To do that, write the query and IntelliSense will open a drop-down menu showing the available options, as shown in Figure 2-23.

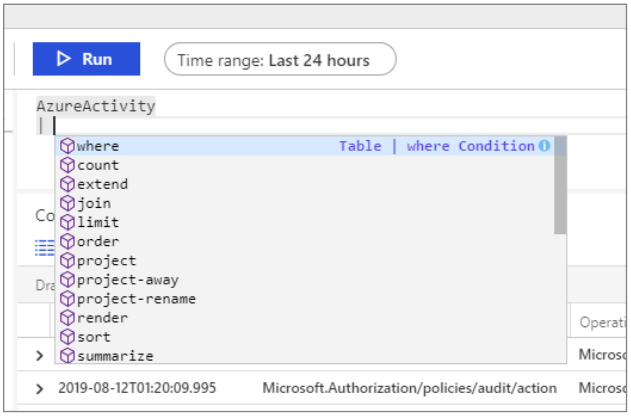


**FIGURE 2-23** Using the context-sensitive IntelliSense capability

To narrow the search to look only for activities that are related to VM creation (which was the task you did in the beginning of this chapter), type the query below and click **Run**.

```
AzureActivity
| where OperationName contains "Create or Update Virtual Machine"
```

The results should be similar to Figure 2-24, unless you have done other activities where the operation name refers to the VM creation or an update to the VM.

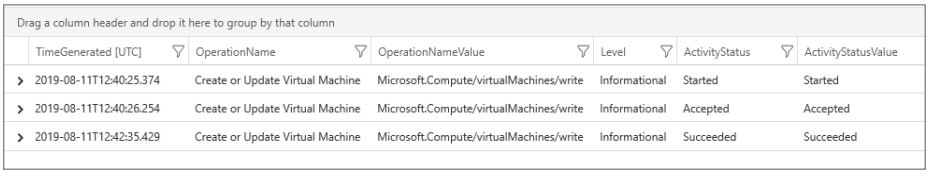


**FIGURE 2-24** Results of a more specific query

To validate the other data sources that were ingested in this chapter, you can use the following sample queries:

- **Azure Active Directory**
  - Query: *SigninLogs*
    - Use this query to visualize all Azure AD sign-in logs.
  - Query: *AuditLogs*
    - Use this query to visualize all Azure AD audit logs.

- **Azure Active Directory Identity Protection**
  - Query: *SecurityAlert | where ProviderName == "IPC"*
    - Azure AD Identity Protection alerts are located under the *SecurityAlert* table, and the way to identity alerts coming from this provider is by using the keyword *"IPC"* on the *ProviderName* field. This query will list all alerts generated by Azure AD Identity Protection.
- **Azure Security Center**
  - Query: *SecurityAlert | where AlertName contains "suspicious"*
    - This query will list all alerts generated by Security Center where the alert name contains the keyword *"suspicious"*.

# Index

## SYMBOLS



## A

## B



## C

## D



## E

## F



## G



## H



## I

## J



## K



## L

# M



# N

## O



## P



## Q



## R

## S



## T

## U



## V



## W